REMARKS

The Office Action dated November 27, 2006 regarding the above-identified application has been carefully considered; and the claim amendments above together with the remarks that follow are presented in a bona fide effort to respond thereto and address all issues raised in that Action. The aggregate verification function has been moved from claim 2 to claim 1, and claim 1 has been amended to clearly recite the digital signature of the aggregate, to distinguish the independent claim over applied art. Other changes have been made in claims 1 and 2 and to dependent claims 6 and 7, for consistency/clarity. New claims 8-14 are added to provide method coverage. Care has been taken to avoid entry of new matter. For reasons discussed below, it is believed that this case is in condition for allowance. Prompt favorable reconsideration of this amended application is requested.

Claims 1, 2 and 4-7 stand rejected under 35 U.S.C. §102(e) as anticipated by U.S. Patent No. 6,671,805 to Brown et al. (hereinafter Brown). Claim 3 stands rejected under 35 U.S.C. §103 as unpatentable over Brown in view of U.S. Application Publication No. 2003/0145197 to Lee et al. (hereinafter Lee). These rejections are traversed.

Before discussing specific distinctions of the claims over the art, it may be helpful first to consider the subject matter disclosed in the present application, by way of an illustrative example. As disclosed in the present application, an electronic document is divided into two or more partial documents (e.g. at step 115 in FIG. 4), and items 302 or 304 of information are generated for verifying validity for the respective partial documents. Examples of the items of information include hash functions 302a-302d for the respective partial documents 300a-300d (step 133 in FIG. 6) and signatures 304a-304d for the respective partial documents 300a-300d (step 134 in FIG. 6). The disclosed technique also involves generating an aggregate of the generated items of information for verifying the validity of all the partial documents (step 135 in

FIG. 6), and generating a digital signature 303a or 303b to the aggregate of the generated items of information (step 136 in FIG. 6). In the illustrated example of FIG. 2, the unmasked data 2 and signature-related data 4a or the unmasked data 2 and signature-related data 4b are combined and saved as the whole data 3. The partial documents may be masked, e.g. so that the electronic document is partially rendered private at the time of its disclosure. However, the validity of the masked electronic document (FIG. 3) can be verified, by verifying the aggregate (302a-302b or 304a-304b) of the generated items of information using the digital signature (303a or 303b; see also steps 144-146 in FIG. 7).

Independent method claim 8 recites, ***inter alia***:

> generating an item of information to verify validity for each of the partial documents;
>
> generating an aggregate of the generated items of information for verifying the validity of all the partial documents;
>
> generating a digital signature to the aggregate of the generated items of information;
>
> ...; and
>
> verifying the validity of the masked electronic document by verifying the aggregate of the generated items of information using the digital signature.

The independent apparatus claim 1 recites functions of the system elements, and the recited functions include functions similar to the above-quoted steps of method claim 8. Although the wording (and thus claim scope) varies somewhat, both independent claims specify generating an item of information to verify validity for each of the partial documents. Each independent claim also recites generating an aggregate of those items and generating a digital signature to the aggregate of the generated items. In both independent claims, the verification of the validity of the masked electronic document is then implemented by verifying the aggregate of the generated items of information using the digital signature. With this approach, for example, it is possible to confirm validity of the whole electronic document even if one or more of the partial documents is masked (e.g. deleted for modified); and it is possible to disclose the electronic documents to the public while leaving it partially undisclosed.

It is respectfully submitted that Brown does not disclose a document management system or method as recited in Applicants' independent claims. The patent discloses a method for digitally signing an electronic document. A signing module 108 calculates a message digest, such as a hash value, for a "to-be-signed" portion within the electronic document; and the digital signature is applied to the message digest (see e.g. column 9, lines 3-30). A receiver of the document can verify the digital signature for the corresponding "to-be-signed" portion (column 22, lines 9-22). Portions of the document may be encrypted for masking purposes, and such a portion also is signed by a person authorized to access such a document portion (column 13, lines 8-12). Brown also suggests adding an encrypted digital certificate, to authenticate the signer (column 14, lines 18-37).

Brown's method can guarantee the validity of each individual "to-be-signed" portion. However, it cannot always verify the electronic document as a whole. If a portion of a different document is added in an unauthorized manner to the targeted document, Brown's method is incapable of verifying the document concerned. If the "to-be-signed" portion is deleted, the method cannot detect the absence of that portion.

It is respectfully submitted that the Brown patent, particularly in the various text sections cited in the rejection, does not teach generating an aggregate of the items of information that were generated for verifying the validity of all the partial documents or generating a digital signature to such an aggregate. The digital signatures of Brown are signatures with respect to to-be-signed or masked portions of the document. Brown's encrypted certificate is for authenticating the signer. Neither of these would be a signature of an aggregate of the items of information for verifying the document portions. As a corollary, the Brown patent does not teach verifying the validity of the masked electronic document by verifying the aggregate of the generated items of information using the digital signature. Hence, Brown does not satisfy a number of limitations of the independent claims, and Brown does not anticipate either independent claim. Claims 1-14 therefore are novel over Brown.

It is respectfully submitted that the combination of Brown and Lee applied in the obviousness (103) rejection also would not satisfy the aggregate generation, signature and verification recitations of claim 1 or claim 8 and therefore does not render either independent claims or any of the dependent claims obvious. Lee was cited in the 103 rejection only for an alleged teaching of a display function. The addition of only a display function to Brown would still result in a system or method of operation which provides signatures with respect to to-be-signed or masked portions of the document and/or or encrypted certificates for authenticating the signers. Such a combination would still not provide an aggregate of the items of information that were generated for verifying the document portions and would not verify the validity of the masked electronic document by verifying the aggregate using the digital signature. Since the proposed combination would not meet the independent claim limitations, the proposed combination does not satisfy all aspects of any of the dependent claims, including rejected claim 3. Applicants therefore submit that the obviousness rejection under 35 U.S.C. § 103 should be overcome.

Upon entry of the above claim amendments, claims 1-14 are active in this application, all of which should be novel and patentable over the art applied in the Action. Applicants therefore submit that all of the claims are in condition for allowance. Accordingly, this case should now be ready to pass to issue; and Applicants respectfully request a prompt favorable reconsideration of this matter.

It is believed that this response addresses all issues raised in the November 27, 2006 Office Action. However, if any further issue should arise that may be addressed in an interview or by an Examiner's amendment, it is requested that the Examiner telephone Applicants' representative at the number shown below.

To the extent necessary, if any, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Keith E. George

/Keith E. George
Registration No. 34,111

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 KEG:apr
Facsimile: 202.756.8087
Date: February 27, 2007

Please recognize our Customer No. 20277 as our correspondence address.